Jaarverslag

Functionaris Gegevensbescherming 2022

Jaarverslag

Functionaris Gegevensbescherming 2022

Opdrachtgever:	gemeente Barneveld Afdeling Bestuur & Dienstverlening
Auteur:	Indra van der Wolf, Functionaris Gegevensbescherming
Datum:	februari 2023

Inhoud

1. MANAGEMENTSAMENVATTING

Dit jaarverslag – dat mede in samenwerking met de Privacy Officer (PO) en de Chief Information Security Officer (CISO) – door de Functionaris Gegevensbescherming (FG) is opgesteld, geeft weer wat de Gemeente Barneveld in 2022 heeft ondernomen om aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) te voldoen.

Het register van verwerkingen is geactualiseerd en er is voor de Wpg een apart register opgesteld. Daarnaast zijn er zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met verwerkers. Ook zijn er intern veel adviezen gegeven en workshops gehouden over privacy en informatieveiligheid, omdat deze onlosmakelijk met elkaar verbonden zijn en het belangrijk is dat het bewustzijn bij de medewerkers aanwezig is en dat ook blijft. Daarbij is niet alleen aandacht besteed aan de grondslag en doelbinding die aanwezig moet zijn voordat gegevens verwerkt mogen worden, welke gegevens verwerkt mogen worden en hoe lang deze bewaard mogen worden, maar ook is het belang onderstreept van een zorgvuldige verwerking en deling van gegevens door bijvoorbeeld gebruik te maken van beveiligd e-mailen.

Sinds de coronapandemie medio maart 2020 wordt door de meeste medewerkers zowel op kantoor als vanuit huis gewerkt. Thuiswerken brengt nieuwe mogelijkheden, maar ook risico’s met zich mee op het gebied van privacy en informatiebeveiliging. Voor de risico’s die thuiswerken met zich meebrengt is aandacht gevraagd.

De gemeente Barneveld heeft de bescherming van privacy en een goede informatieveiligheid hoog in het vaandel staan. Veel is goed geregeld. Om dit zo te houden, dient er continue aandacht besteed te worden aan privacy van burgers, bedrijven en medewerkers, waarbij een zorgvuldige verwerking van de persoonsgegevens en de bescherming daarvan steeds gewaarborgd moet zijn. Het jaar 2022 stond, evenals 2021, in het teken van borging, waarbij de verwerking van persoonsgegevens en de bescherming daarvan nog beter verankerd zal worden in de organisatie door middel van protocollen, procedures, bewustzijnsacties, waar nodig aanpassingen in applicaties en software, en dat de medewerkers zich daarvan bewust zijn en ook daarnaar handelen.

Daarnaast is in 2022 aandacht besteed aan de evaluatie van de eerder gecommuniceerde aanbevelingen en te nemen maatregelen om de verwerking van persoonsgegevens en onder andere de bewaartermijnen beter te borgen en na te leven. Verder is in 2021 een evaluatie gestart over het gebruik van cameratoezicht in het centrum van Barneveld. De verantwoordelijkheid voor de camera's ligt bij de politie, evenals het uitvoeren van een DPIA met betrekking tot de inzet van cameratoezicht en de beoordeling of dit cameratoezicht noodzakelijk is en voortgezet moet worden.

Tot slot zijn in 2022 een interne en externe audit uitgevoerd voor de Wpg. Op grond van de Wpg moet elk jaar een interne audit worden uitgevoerd en één keer per vier jaar een externe audit. De audits hebben betrekking op de verwerking van politiegegevens door de buitengewone opsporingsambtenaren openbare ruimte en de leerplichtambtenaren. Uit de audits zijn een aantal verbeterpunten naar voren gekomen, die binnen een jaar doorgevoerd moeten worden. De rapportage over de externe audit moest daarnaast voor 31 december 2022 zijn ingediend bij de Autoriteit Persoonsgegevens (AP), aan deze verplichting heeft de gemeente Barneveld voldaan.

2. WETTELIJK KADER

2.1 AVG Algemeen

In de AVG zijn regels vastgelegd voor het verwerken van persoonsgegevens. Deze verordening voor de verwerking van persoonsgegevens kent een rechtstreekse werking voor de lidstaten van de Europese Unie. In de AVG worden de rechten van burgers versterkt en de AVG legt de nadruk op de eigen verantwoordingsplicht van organisaties die persoonsgegevens verwerken. Dit betekent dat organisaties bijvoorbeeld goed moeten vastleggen welke gegevens zij verwerken, met welk doel, hoe lang zij die gegevens bewaren, dat zij de gegevens goed beveiligen en met wie ze gegevens delen. De rechtstreekse werking van de AVG zorgt ervoor dat de regels voor bescherming van persoonsgegevens uniform zijn binnen de Europese Unie.

De AVG geeft een overkoepelend kader voor het verwerken van persoonsgegevens en is nader uitgewerkt in de Nederlandse Uitvoeringswet AVG. Daarnaast zijn er in materiewetgeving, zoals de Jeugdwet, de Wet maatschappelijke ondersteuning, de Wet Basisregistratie personen specifieke regels te vinden voor het verwerken van persoonsgegevens. De AVG hangt daar altijd als een paraplu boven. Dat betekent dat als persoonsgegevens verwerkt mogen worden op grond van de materiewetgeving, de bepalingen van de AVG daarboven blijven hangen. Er moet bijvoorbeeld altijd een rechtmatige grondslag zijn voor het verwerken van persoonsgegevens en persoonsgegevens mogen alleen worden verwerkt voor het doel waarvoor ze zijn verzameld.

2.2 Wet politiegegevens

Buitengewone opsporingsambtenaren (boa's) die voor hun opsporingstaak persoonsgegevens verwerken, vallen onder de Wpg. Boa's verwerken de politiegegevens onder beheer van hun werkgever en daarmee is de werkgever van de boa's de verwerkingsverantwoordelijke. Voor de gemeente Barneveld geldt dat zij als werkgever boa's openbare ruimte en leerplichtambtenaren in dienst heeft die bij het uitvoeren van hun taken politiegegevens verwerken. Als gemeente zijn wij daarom verantwoordelijk voor het toezicht op de naleving van de Wpg. In de Wpg is ook een auditverplichting opgenomen voor werkgevers van boa's.

- Interne Wpg-audit: elk jaar. Dat betekent dat de werkgever van die boa's verplicht is om elk jaar een interne Wpg-audit te doen.
- Externe Wpg-audit: elke vier jaar. De werkgever moet elke vier jaar een externe Wpg-audit laten uitvoeren en de resultaten daarvan aan de Autoriteit Persoonsgegevens (AP) sturen.

2.3 Specifieke wetgevende ontwikkelingen, jurisprudentie en nieuwsberichten van de Autoriteit Persoonsgegevens

2.3.1 Contouren algoritmetoezicht AP naar Tweede Kamer

Staatssecretaris Alexandra van Huffelen (Digitalisering) heeft de Tweede Kamer nader geïnformeerd over het in te richten algoritmetoezicht bij de Autoriteit Persoonsgegevens (AP)[1]. In de Kamerbrief staat met welke nieuwe activiteiten de AP, samen met de andere colleges, markttoezichthouders en rijksinspecties, in 2023 aan de slag gaat. Daarnaast wordt het al bestaande toezicht op algoritmes die (onrechtmatig) persoonsgegevens verwerken in 2023 versterkt.

Met het algoritmetoezicht bij de AP geeft Van Huffelen invulling aan de ambitie van de Tweede Kamer en het kabinet om te regelen dat algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur en dat dat wordt bewaakt door de AP. Een belangrijk onderdeel van het nieuwe toezicht is het signaleren en analyseren van sector- en domeinoverstijgende risico's van algoritmes, en de samenwerking met andere organisaties te faciliteren en te intensiveren. Vanaf januari start de AP met deze nieuwe activiteiten. De focus ligt daarbij in de beginperiode op het signaleren van risicovolle algoritmes, het bundelen van kennis en het verder vormgeven van de samenwerking.

2.3.2 Handreiking Autoriteit Persoonsgegevens voor gemeenteraadsleden

De Autoriteit persoonsgegevens (AP) heeft voor gemeenteraadsleden tips gepubliceerd voor het controleren van de inzet van technologie en het deelnemen aan samenwerkingsverbanden. Deze handreiking is een aanvulling op de eerder uitgebrachte handreiking "Gemeenten en privacy: wat kunt u als raadslid doen?". Beide handreikingen kunnen raadsleden helpen bij het stellen van de juiste vragen over privacy binnen hun gemeente[2]. Deze handreiking is ook met raadsleden gedeeld tijdens de Informatiecarrousel raadsleden op 10 oktober 2022. De handreiking staat hier.

2.3.3 Doorgifte persoonsgegevens aan kerken

De AP heeft in een advies aan het kabinet gesteld dat de overheid kerken niet meer zomaar persoonsgegevens van kerkleden moet doorsturen uit de administratie van de

[1] Contouren algoritmetoezicht AP naar Tweede Kamer | Autoriteit Persoonsgegevens
[2] AP helpt raadsleden bij controleren inzet technologie en samenwerkingsverbanden in gemeenten | Autoriteit Persoonsgegevens en AP biedt raadsleden handreiking AVG | Autoriteit Persoonsgegevens

overheid, de Basisregistratie Personen (BRP)[3]. Organisaties krijgen toegang tot de BRP voor bepaalde overheidstaken of als zij een groot maatschappelijk belang dienen.

Geen groot maatschappelijk belang
De AP concludeert in het wetgevingsadvies over het experiment dat het zonder toestemming doorgeven van persoonsgegevens uit de BRP aan kerken niet mag. En dat dit geldt voor alle kerkleden, dus ook voor mensen die al langer lid zijn van een kerk. Het doorgeven van persoonsgegevens uit de BRP aan de kerken dient namelijk geen algemeen belang en is niet noodzakelijk. Naar mening van de AP strookt dit niet met de AVG en moet het stoppen. Overigens verstrekt de gemeente Barneveld geen gegevens aan kerken.

2.3.4 Gebruiken van persoonsgegevens uit overheidsdata

De AP adviseert het voorstel voor een wijziging van de Wet hergebruik van overheidsinformatie aan te passen[4]. Het voorstel, waarin het kabinet overheidsinstellingen aanmoedigt overheidsdata, inclusief persoonsgegevens, beschikbaar te stellen voor hergebruik, stelt onvoldoende grenzen. Met het risico dat persoonsgegevens worden gedeeld zonder toestemming of medeweten van de mensen om wie het gaat.

Het wetsvoorstel moet ervoor zorgen dat zoveel mogelijk overheidsdata beschikbaar worden gesteld, bijvoorbeeld voor onderzoek, maar ook voor commercieel gebruik. Die data moeten volgens het voorstel ook doorzoekbaar zijn met software en te combineren zijn met andere data. Overheidsinstellingen worden verzocht informatie openbaar te maken, tenzij zij zelf inschatten dat dat niet kan.

In haar advies aan het kabinet pleit de AP ervoor om in de wet op te nemen dat hergebruik van persoonsgegevens in openbare registers in principe verboden is. En vervolgens in regels vast te leggen wanneer welke persoonsgegevens wél voor hergebruik beschikbaar mogen worden gesteld, en dus een uitzondering zijn op dat verbod. In de regels moet ook rekening worden gehouden met de vrijheid van mensen om hun gegevens toch voor hergebruik beschikbaar te laten stellen.

2.3.5 Wpg– audit

Werkgevers van boa's met opsporingstaken zijn verplicht om jaarlijks een interne audit uit te voeren[5]. Ook is er elke vier jaar een externe audit nodig. Dat staat in de Wpg. De resultaten van de externe audit moeten boa-werkgevers naar de AP sturen. Na een jaar uitstel, ligt de uiterste datum voor het aanleveren van Wpg-auditrapporten op 31 december 2022, dit betreft de externe audit over het jaar 2021. Maar de AP ziet dat er nog weinig rapporten binnen zijn, en benadrukt het belang van het tijdig uitvoeren, rapporteren en toezenden van de audit.

[3] AP: ongevraagd doorgeven persoonsgegevens aan kerken moet stoppen | Autoriteit Persoonsgegevens
[4] AP: stel grenzen aan opnieuw gebruiken van persoonsgegevens uit overheidsdata | Autoriteit Persoonsgegevens
[5] Nog weinig boa-werkgevers hebben verplichte Wpg-audit aangeleverd | Autoriteit Persoonsgegevens

Uit een nieuwsbericht van 12 januari 2023 van de AP blijkt dat veel werkgevers van boa's de resultaten van de verplichte Wpg-audit niet of te laat hebben toegestuurd[6]. De AP gaat deze organisaties om tekst en uitleg vragen. Op 31 december 2022 had de AP van ruim 600 boa-werkgevers een auditrapport moeten hebben ontvangen. De teller bleef steken op een derde daarvan. De gemeente Barneveld heeft tijdig de auditrapportage toegezonden aan de AP.

2.4 TOEZICHTSKADER AP: ONTWIKKELINGEN EN GEVOLGEN

De AP heeft in november 2019 haar toezichtkader voor de jaren 2020 tot en met 2023 gepubliceerd. In dit kader geeft de AP haar prioriteiten aan voor de komende jaren.

De AP legt de komende jaren in het toezichtwerk extra nadruk op drie focusgebieden: datahandel, digitale overheid en artificiële intelligentie en algoritmes. Dat maakte de AP op 11 november 2019 bekend met het visiedocument 'Dataprotectie in een digitale samenleving'. Extra nadruk op deze thema's is nodig om de bescherming van persoonsgegevens in Nederland te borgen. Misbruik of onverantwoordelijk gebruik van persoonsgegevens kan bijvoorbeeld leiden tot foutieve beslissingen, uitsluiting van mensen en discriminatie. Tot en met 2023 geven de focusgebieden onder meer richting aan de uitvoering van de wettelijke taken van de AP.

Trends en ontwikkelingen
De AP ziet drie grote trends die van invloed zijn op de bescherming van persoonsgegevens:

- Doorgroei van de datasamenleving
- Toename van digitaal onrecht
- Toename van privacybewustzijn

Focusgebieden
In vervolg op de gesignaleerde trends kiest de AP voor drie focusgebieden:

Datahandel
Data maken producten en diensten slimmer en deze producten en diensten creëren vervolgens weer meer data. Dit heeft voordelen, maar ook nadelen: er vindt steeds meer ongeoorloofde doorverkoop plaats van persoonsgegevens aan derden. Mensen verliezen hierdoor steeds meer grip op hun gegevens en daarmee op hun leven.

Digitale overheid
Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens. De overheid werkt gericht aan het inzetten van persoonsgegevens. Het is van belang dat

[6] AP treedt op tegen boa-werkgevers die verplichte Wpg-audit niet toesturen | Autoriteit Persoonsgegevens

de overheid verantwoordelijk omgaat met persoonsgegevens, zodat mensen niet onnodig in de knel kunnen komen.

Artificiële Intelligentie en algoritmes
Steeds meer bedrijven en organisaties maken gebruik van algoritmes en AI. Dit biedt voordelen en leidt tot nieuwe nuttige toepassingen. Maar de inzet van AI en algoritmes kent ook risico´s en schadelijke effecten. Onverantwoordelijk gebruik van algoritmes kan leiden tot foutieve beslissingen, tot uitsluiting van mensen en tot discriminatie. De AP is als toezichthouder verantwoordelijk voor het toezicht op de verwerking van persoonsgegevens, en daarmee ook op de toepassing van AI en algoritmes waarbij persoonsgegevens worden gebruikt.

Deze thema's passen bij de missie van de AP en spelen in meerdere sectoren. De AP kan hier het verschil maken door grenzen te markeren ten aanzien van wat er wel en niet kan onder de AVG. De focusgebieden geven onder meer richting aan de uitvoering van de wettelijke taken van de AP. Daarnaast houdt de AP oog voor actuele ontwikkelingen.

Risicogestuurd toezicht
De AP is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Het toezichtveld is omvangrijk: internationale en nationale bedrijven en organisaties, de gehele overheid, inclusief politie en justitie en ook verenigingen, scholen, stichtingen en individuele burgers.

De AP houdt daarom risicogestuurd toezicht. Dat betekent dat de AP is gespitst op onderwerpen met een groot risico voor burgers. Daarbij weegt de AP af om hoeveel data het gaat en hoe gevoelig die data zijn. Op basis daarvan gebruikt de AP een of meerdere toezichtsinstrumenten, zoals normuitleg, wetgevingsadvies, voorlichting of handhaving.

3. GOVERNANCE

3.1 Governance algemeen

Er is een duidelijke structuur aangaande de governance aanwezig wat betreft de uitvoering van de AVG. Er zijn een Chief Information Security Officer (CISO), een Privacy Officer (PO) en een Functionaris Gegevensbescherming (FG) aangewezen door het college. Deze onderlinge relaties en verantwoordingen blijken uit het door het college vastgestelde en op 1 april 2018 in werking getreden Privacybeleid. Dit beleid is in 2021 herzien, op 11 mei 2021 door het college vastgesteld en op 1 juni 2021 in werking getreden. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient aan te kunnen tonen 'in control' te zijn aangaande de uitvoering van de AVG.

3.2 Verantwoording Functionaris gegevensbescherming

Overzicht uitgevoerde werkzaamheden in 2022:

- In 2022 zijn er een aantal Data Protection Impact Assessments (DPIA's) uitgevoerd vanwege nieuwe processen, herziening van de DPIA of vanwege aanschaf of uitbreiding van een applicatie. De rapportages van deze DPIA's zijn gedurende 2022 en een enkele begin 2023 afgerond, zodat het tweede en derde kwartaal van 2023 gebruikt kunnen worden om de uit de DPIA's voortvloeiende acties op te pakken en uit te voeren.
- Het Register van Verwerkingen is in 2023 geactualiseerd en er is een register voor de Wpg opgesteld.
- In het voorjaar van 2021 is het borgingsdocument dat VNG en IBD hebben ontwikkeld, herzien en anders vormgegeven. Begin januari 2023 is aan de hand van het IBD borgingsdocument de borging van privacy en informatiebeveiliging beoordeeld en zijn de resultaten geëvalueerd ten opzichte van het jaar daarvoor. De daaruit voortkomende acties worden in 2023 opgepakt. Zie verder bij 3.5.
- Voor de Wpg is een interne en externe audit uitgevoerd en wordt naar aanleiding hiervan in 2023 een verbeterplan opgesteld. De punten uit dit verbeterplan worden ook in 2023 opgepakt.

3.3 Verantwoording Privacy Officer

Overzicht uitgevoerde werkzaamheden in 2022:

DPIA's uitvoeren	In 2022 zijn een aantal DPIA's uitgevoerd op risicovolle processen, waaronder de overgang naar een nieuw zaaksysteem, de personeels- en salarisadministratie en de uitvoering van de Wet Damocles.
Overige vereisten uit de AVG invoeren	Privacy by design en default zijn vanaf mei 2018 bij nieuwe applicaties als eis meegenomen. Dit wordt onder meer vormgegeven door deelname aan het Planatelier en het pro- actief handelen van collega's door de PO vroegtijdig te betrekken.
Bewustwording privacy en informatiebeveiliging	- Er zijn digitale workshops voor (nieuwe) medewerkers verzorgd. - Periodiek is een nieuwsbericht op intranet gezet.
Wet politiegegevens	Door de PO is, in samenwerking met de inhoudelijke collega's een interne audit uitgevoerd op de verwerking van politiegegevens. Daarnaast is een externa audit uitgevoerd, deze is door de PO gecoördineerd.
Privacy en Publiekszaken	In overleg met Publiekszaken is ondersteuning geboden bij privacyvraagstukken (verstrekken gegevens uit de BRP).

Instellen + vullen register van verwerkingen	Nieuwe processen worden toegevoegd en wijzigingen in processen worden in het register doorgevoerd. Daarnaast is het register aangepast op de nieuwe organisatiestructuur van de gemeente.
Ondersteunen bij ontwikkelingen dienstverlening	Bij het ontwikkelen van nieuwe/ andere vormen van de dienstverlening van Barneveld is de privacyregelgeving meegenomen en neemt waar nodig de PO deel aan (implementatie) projecten.
Inzageverzoeken	De meeste verzoeken tot recht van inzage hebben betrekking op het sociaal domein en deze zijn samen met de betrokken gespreksvoerder en de Privacy Officer afgehandeld.
Proces omtrent datalekken inregelen en monitoren	Inbreuken in verband met privacy zijn geregistreerd. Datalekken zijn gemeld bij de AP.
Overige werkzaamheden	Naast de hierboven genoemde werkzaamheden zijn door de PO de volgende werkzaamheden verricht: - Toetsen/ opstellen verwerkersovereenkomsten - Toetsen/ opstellen convenanten - Behandelen privacyvraagstukken - Signaleringsfunctie in organisatie - Sparringpartner voor de organisatie

3.4 Verantwoording CISO

In juni 2022 heeft gemeente Barneveld een vaste CISO aangetrokken. Overzicht van uitgevoerde werkzaamheden in 2022:

Bewustwording privacy en informatiebeveiliging	- Samen met de PO zijn workshops voor medewerkers verzorgd. - Op verzoek zijn de CISO of PO bij teamoverleggen aanwezig geweest. - De CISO neemt periodiek deel aan afdelingsoverleggen binnen I&A. - Met campagnemateriaal is bewustwording gecreëerd. - Periodiek is een nieuwsbericht op intranet gezet. - Tegen het eind van 2022 is een enquête uitgevoerd m.b.t. het niveau van bewustzijn rond informatiebeveiliging. De resultaten daarvan worden in februari 2023 verwacht.
Zelfevaluatie BRP/PNIK	Jaarlijks draagt de gemeente verantwoording af over informatiebeveiliging rond BRP / Pnik.
Zelfevaluatie ENSIA	Jaarlijks draagt de gemeente verantwoording af over informatiebeveiliging door middel van ENSIA (Eenduidige Normatiek Single Information Audit). Hierin vallen onder andere BAG, BGT, DigiD, Suwinet en BIG. Daarbij worden DigiD, Suwinet en de ENSIA-verantwoording getoetst door een externe RE/RA auditor.

BIO	Controleren en evalueren van de huidige set maatregelen.
Pentests	Er zijn twee penetratietests uitgevoerd, waarvan één met focus op de fysieke omgeving. De uitkomsten van de pentests zijn verwerkt in veranderingen, projecten en gebruik van nieuwe tooling.

3.5 Borging

De VNG en IBD hebben samen begin 2021 een vernieuwd borgingsdocument opgesteld, die bestaat uit quickscans en controlevragen. De quickscans kunnen worden gebruikt om snel te meten waar de organisatie staat op de diverse thema's. Vervolgens kan een verdiepingsslag worden gemaakt met de control-vragenlijsten, opgesplitst in O- controls en P-controls. O ziet op organisatiemaatregelen en P ziet op procesmaatregelen. De vragen zijn opgesplitst in 7 onderdelen: beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording.

Voor het jaar 2022 is de control vragenlijst uitgevoerd door de PO, CISO en FG. Hieruit is af te leiden dat de Gemeente Barneveld goed in zicht heeft op wat wel, niet of deels geregeld is en waar nog aandacht aan besteed moet worden. Bij zaken die de score gedeeltelijk hebben gekregen, is de betreffende zaak veelal wel goed ingeregeld, maar ontbreekt een vastlegging van ongeschreven gedragsregels.

Verder is bij nog niet iedere applicatie logging en monitoring ingeregeld of zijn zaken niet automatisch maar alleen handmatig te wijzigen. De oorzaak hiervan ligt soms in het feit dat het om oudere applicaties gaat waarbij dat lastiger is in te regelen. Bij alle applicaties die onlangs zijn aangeschaft of nog worden aangeschaft wordt vooraf al een programma van eisen opgesteld, zodat er sprake is van privacy by design en privacy by default. Hierdoor wordt dan niet geheel aan de norm voldaan of is het volwassenheidsniveau minder hoog, omdat de norm en het volwassenheidsniveau over de gehele gemeente wordt gemeten.

Tot slot worden een aantal zaken die op gedeeltelijk staan in de actualisering van beleid en de opstelling van nieuw beleid meegenomen. Overigens kan opgemerkt worden dat een 100% score nooit te garanderen is, omdat privacy & security vakgebieden zijn die continue in beweging zijn.

4. WERKZAAMHEDEN EN BEVINDINGEN

4.1 Privacybeleid

Op 1 april 2018 is het Privacybeleid in werking getreden. Op 30 mei 2018 is de gemeenteraad hierover geïnformeerd. Dit beleid implementeert de uitgangspunten en verplichtingen uit de AVG. De uitgangspunten rechtmatigheid, behoorlijkheid, transparantie, doelbinding, subsidiariteit, proportionaliteit, dataminimalisatie en vertrouwelijkheid worden omgezet in alle werkprocessen waarbinnen

persoonsgegevens worden verwerkt. Er is beleid gevormd op hoe om te gaan met de rechten van betrokkenen, meldplicht datalekken, de functies van FG, PO en CISO en de gegevensuitwisseling tussen verschillende domeinen en afdelingen.

Het nieuwe privacybeleid is op 11 mei 2021 vastgesteld door het college en is op 1 juni 2021 in werking getreden. De raad is hierover geïnformeerd en ook op de website is hier aandacht aan besteed.

4.2 Thuiswerken

In 2022 waren er ook nog landelijk maatregelen afgekondigd ter bestrijding van Covid- 19. Bij de Gemeente Barneveld zijn toen ook lokaal maatregelen getroffen. Een daarvan was het thuiswerken voor alle medewerkers, tenzij dat niet mogelijk was vanwege de aard van de werkzaamheden (zoals (deel) publiekszaken, afvalophaaldienst, groenvoorziening e.d.).

Nu de Covid- 19 pandemie voorbij is, wordt door de meeste medewerkers zowel op kantoor als vanuit huis gewerkt. Thuiswerken brengt nieuwe mogelijkheden, maar ook risico's met zich mee op het gebied van privacy en informatiebeveiliging. Voor de risico's die thuiswerken met zich meebrengt is aandacht gevraagd.

Er is benadrukt dat de regels van privacy en informatiebeveiliging in acht genomen moeten worden. Vanuit privacy is aangegeven dat het ongewenst en ook strijdig met het privacybeleid is dat medewerkers fysieke documenten meenemen met daarop persoonsgegevens of andere vertrouwelijke gegevens. Via de beveiligde netwerkomgeving zijn alle documenten beschikbaar.

Vanuit informatieveiligheid/-beveiliging zijn de regels voor thuiswerken nogmaals onder de aandacht gebracht, ook middels de verplichte workshops. Daarbij zijn medewerkers erop geattendeerd dat ze met vertrouwelijke gegevens en informatie werken.

4.3 Wpg- audit

Op grond van de Wpg moet elk jaar een interne audit worden uitgevoerd en één keer per vier jaar een externe audit. In 2022 zijn er zowel een interne als een externe audit uitgevoerd voor de Wpg over het jaar 2021. De audits hebben betrekking op de verwerking van politiegegevens door de buitengewone opsporingsambtenaren openbare ruimte en de leerplichtambtenaren. Uit de audits zijn een aantal verbeterpunten naar voren gekomen, die binnen een jaar doorgevoerd moeten worden. Hiervoor wordt begin 2023 een verbeterplan opgesteld en de actiepunten hieruit worden opgepakt en uitgevoerd voor november 2023. In november vindt vervolgens een hercontrole door een de partij die de externe audit heeft uitgevoerd.

De rapportage over de externe audit moest daarnaast voor 31 december 2022 zijn ingediend bij de Autoriteit Persoonsgegevens (AP), aan deze verplichting heeft de gemeente Barneveld voldaan.

4.4 Register van verwerkingen

In 2022 is het register van verwerkingen geactualiseerd. Bij alle verwerkingen die in het register zijn opgenomen, worden de bewaartermijnen gehanteerd zoals deze door de VNG zijn vastgesteld in de "Selectielijst 2020".

Nieuwe verwerkingen zijn in het register opgenomen en gewijzigde verwerkingen zijn aangepast. Daarnaast is de nieuwe organisatiestructuur in het register opgenomen.

Daarnaast zijn in het register verwerkingen aangepast dan wel toegevoegd, om een duidelijk onderscheid te maken tussen verwerkingen op grond van de AVG en verwerkingen op grond van de Wpg.

4.5 Meldingen datalekken

Informatiebeveiligingsdienst: Het jaar in cijfers
De Informatiebeveiligingsdienst (IBD) ontving het afgelopen jaar 2.313 aanvragen- en meldingen over informatiebeveiliging en 467 privacy- aanvragen. De IBD registreerde 387 incidenten met een hulp-, coördinatie- of ondersteuningsvraag van gemeenten.

De IBD-CERT verstuurde 1.102 kwetsbaarheidsmeldingen waarvan 62 met een hoge kans op misbruik en een grote potentiële schade. De SMS-waarschuwing werd in 2022 één keer ingezet vanwege een ernstige kwetsbaarheid bij alle gemeenten.

Cijfers Barneveld
In totaal zijn er in 2022 26 beveiligingsincidenten gemeld bij de Gemeente Barneveld. Hiervan zijn drie incidenten gemeld bij de AP. De AP registreert alle meldingen die door gemeenten gedaan worden. De AP reageert alleen in gevallen dat zij 'nader onderzoek' willen doen naar een door de gemeente gedane melding. In 2022 is daarvan geen sprake geweest. Ook heeft de AP geen waarschuwing gedaan of een dwangsom opgelegd aan de Gemeente Barneveld.

Bij geen enkel incident waren de risico's dermate hoog dat het verplicht was om een melding aan de betrokkenen te doen. Desondanks is bij twee incidenten vanuit klantgerichtheid wel gekozen om betrokkenen te informeren. Uit een analyse van de datalekken is gebleken dat het van belang is om blijvend aandacht te besteden aan bewustwording over omgang met bedrijfsmiddelen en/of verwerken van persoonsgegevens. Waar nodig zijn er technische maatregelen getroffen om de gebruikers te ondersteunen.

4.6 Rechten van betrokkenen

Er zijn in 2022 9 verzoeken binnengekomen. Dit betrof 9 inzageverzoeken waarbij bij 2 verzoeken ook sprake was van een verzoek tot verwijdering. Alle verzoeken zijn toegewezen. De meeste verzoeken hebben betrekking op het Sociaal Domein en zijn bijvoorbeeld gericht op het verkrijgen van een second opinion.

Oorspronkelijk zijn in 2022 meer dan 9 verzoeken ingediend, maar na telefonisch contact blijkt veelvuldig dat een verzoek niet als inzageverzoek is bedoeld, maar meer een informatievraag is. Vaak gaat het dan om informatievragen die betrekking hebben op publiekszaken of informatie die personen zelf kunnen opzoeken. Na telefonisch contact blijkt dan geen sprake te zijn van een inzageverzoek en wordt de vraag indien nodig doorgezet naar de juiste afdeling. In 2022 zijn geen klachten ingediend.

4.7 Bewaartermijnen

In 2019 zijn digitale bezemdagen georganiseerd in verschillende teams en zijn teams actief gewezen op het opschonen van mappen op netwerkschrijven en in e-mailboxen. Door de coronapandemie is er door de meeste medewerkers veel thuis gewerkt, waardoor het digitaal bezemen een lagere prioriteit heeft gekregen dan het goed beveiligd thuiswerken. Eind 2021 is het digitaal bezemen weer door enkele teams opgepakt en dit zal in 2023 ook weer onder de aandacht worden gebracht. Inmiddels is iedereen gewend geraakt aan het thuiswerken en weet men met welke privacy en informatiebeveiligings- aspecten rekening gehouden moet worden.

4.8 Verwerkers en verwerkersovereenkomsten

Van alle leveranciers waarmee een verwerkersovereenkomst is afgesloten is een actueel overzicht. Bestaande verwerkers hebben niet gerapporteerd over incidenten. Verder weten collega’s ook de Privacy Officer te vinden als ze twijfelen of een verwerkersovereenkomst moet worden afgesloten en wordt een af te sluiten verwerkersovereenkomst ook altijd voorgelegd aan de Privacy Officer.

Er is in 2022 in een aantal gevallen afgeweken van de standaard en door VNG/IBD verplicht gestelde verwerkersovereenkomst. Dat is gedaan bij zeven verwerkersovereenkomsten. In zes van deze overeenkomsten is artikel 7 anders dan standaard geformuleerd. Artikel 7 verwijst voor het opschonen van gegevens na afloop van de hoofdovereenkomst naar de hoofdovereenkomst. In de genoemde overeenkomsten was het opschonen van gegevens echter niet geregeld in de hoofdovereenkomst. Bij één verwerkersovereenkomst is de standaard van de leverancier (Rijksoverheid) gebruikt.

4.9 Privacy in het Sociaal Domein

Tussen de afdeling Sociaal Domein, voornamelijk de juristen, de beleidsmedewerkers en de informatieadviseur, en de Privacy Officer is een goede samenwerking ontstaan. Indien nodig wordt tijdig de Privacy Officer geraadpleegd en om advies gevraagd.

Met ketenpartners waarmee de gemeente Barneveld samenwerkt of opdrachtgever voor is binnen het Sociaal Domein, wordt per proces beoordeeld of er een overeenkomst moet worden afgesloten en zo ja, wat voor een overeenkomst. Dit kan een verwerkersovereenkomst, een convenant of een andere vorm van een overeenkomst zijn om de privacy te waarborgen. Hierbij wordt nauw en in goed overleg samengewerkt met de teams van het Sociaal Domein.

4.10 Informatieveiligheid

De CISO is druk bezig geweest met het opleveren van de verantwoordingen in het kader van BAG, BGT, DigiD, Suwinet, BIG, ENSIA, BRP en PNIK. Daarnaast zijn er tal van maatregelen geëvalueerd (en eventueel bijgestuurd). De CISO acteert op alle lagen van de Gemeente Barneveld (Strategisch, Tactisch en Operationeel). De CISO stelt zowel beleidsstukken op als dat de CISO langs verschillende teams gaat voor bewustwordingstrainingen.

4.11 Data Protection Impact Assessments

In 2022 zijn er 11 DPIA's voor de onderstaande processen uitgevoerd, waarbij dit voor de meeste processen een herziening en verdieping van de DPIA uit 2018 of 2019 betreft:

1	Zaaksysteem	Invoering nieuw zaaksysteem
2	Veiligheid	RIEC IS
3	Veiligheid	Damocles
4	Personeelszaken	AFAS (personeelsdossier)
5	Woonurgentie	Woonurgentieverklaring
6	Belastingen	Heffingen- en invorderingsadministratie
7	Belastingen	Kwijtschelding gemeentelijke belastingen
8	Handhaving	Bodycams BOA's (Handhaving)
9	Handhaving	BOA verwerkingen Citycontrol
10	Onderwijs	Leerlingenvervoer (melding en aanvraag)
11	Onderwijs	Uitvoering Leerplichtwet en RMC- wet

In 2023 zullen er 7 DPIA's voor de onderstaande processen worden uitgevoerd, waarbij dit voor de meeste processen een herziening en verdieping van de DPIA uit 2019/2020 betreft:

1	Schuldhulpverlening	Vroegsignalering schuldhulp voorafgaand
		Schuldhulpverlening
2	Jeugdzorg	Jeugdzorg
		MDO-lokaal
3	Beveiligingscamera's	Beveiligingscamera's stations en toiletten
4	Horeca-aanvragen	Horeca aanvragen
5	Wmo	Wmo materiele hulp
		Wmo niet materiele hulp
6	Participatiewet	IOAW en IOAZ uitkering
		Participatiewet (uitkering levensonderhoud, bijzondere bijstand, minimaregelingen)
		Participatiewet (re-integratie)
7	Telefonie- en contactcentrum	Invoering nieuw systeem voor klantcontacten

De DPIA's vonden plaats aan de hand van een vragenlijst. Deze vragenlijst is deels gebaseerd op de vragenlijst van de beroepsvereniging voor IT-auditors NOREA en door de privacy officer aangepast en verder aangevuld. Hierin wordt gevraagd naar de verwerkingsverantwoordelijke en verwerkers(overeenkomsten), nieuwe technieken, noodzaak van gegevensverwerking, aard van de persoonsgegevens (bijzonder of gevoelig), gegevensuitwisseling intern en extern, doelbinding, grondslag, transparantie, actualiteit, integriteit en beschikbaarheid van persoonsgegevens, rechten van betrokkenen, bewaartermijnen en beveiliging.
Per proces wordt een rapportage opgesteld met bevindingen, conclusies en aanbevelingen.

In de gehouden DPIA's komen de volgende risico's naar voren:

1. De aanwezigheid van een schaduwarchief. Als de gegevens (gegevens en alle documenten) te lang worden bewaard, houdt dit in dat er een risico is op onrechtmatig gebruik (voor andere doelen) of verlies van gegevens.
2. Er worden gegevens onbeveiligd verzonden per e-mail.
3. Logging en monitoring gebeurt nog onvoldoende.

De volgende maatregelen zijn reeds genomen:

1. Diverse teams hebben hun (schaduw)archieven en mappen (fysiek en digitaal) opgeschoond en belangrijke stukken laten archiveren.
2. Er wordt steeds meer beveiligd gemaild met een wachtwoord.

Er zijn afspraken gemaakt over de termijn waarop andere maatregelen worden genomen.

4.12 Bewustwording

Net als in voorgaande jaren, zijn er in 2022 workshops over Privacy en Informatiebeveiliging gehouden. Deze workshop is verplicht voor alle nieuwe medewerkers en wordt sinds 2022 in kleinere groepen gehouden voor een betere interactie. Belangrijk voor de bewustwording is ook de bekendheid en benaderbaarheid van de PO om als vraagbaak te fungeren. Hiervan is en wordt veel gebruik gemaakt.

4.13 Overige zaken

Ook in 2023 of 2024 zijn er wetswijzigingen te verwachten, waarin gegevensverwerking voorkomt.

Verzamelwet Gegevensbescherming
De Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) krijgt een update en deze treedt in februari 2023 in werking. De UAVG is een verlengstuk van de AVG. Verschillende andere wetten verwijzen ook naar de UAVG en deze wetten worden ook aangepast om ze beter op de AVG en de UAVG af te stemmen.

De wijzigingen zijn:

- Meer rechten voor kinderen tussen 12 en 16 jaar.
- Aanpassing aan de uitleg van het begrip strafrechtelijke persoonsgegevens.
- Grondslag voor accountants en curatoren om bijzondere persoonsgegevens en/ of strafrechtelijke persoonsgegevens te verwerken.
- Het gebruik van biometrische gegevens met het doel om toegang te krijgen tot bepaalde plaatsen, diensten, informatiesystemen, etc.
- Bij het pensioen of overlijden van een hulpverlener wordt de overdracht van dossiers naar een andere hulpverlener, die ze gedurende de wettelijke bewaartermijn bewaart, beter geregeld.

Algoritmeregister
Sinds december 2022 zijn ruim honderd algoritmes die de overheid gebruikt in een online-register samengebracht in het Algoritmeregister. De nieuwe site moet zorgen voor meer transparantie over de algoritmes die overheden inzetten. Ministeries, gemeenten en andere takken van de overheid kunnen hun algoritmes delen op het Algoritmeregister, maar dat is nog niet verplicht. De Tweede Kamer wil wel dat dit gebeurt. De verwachting is dat een dergelijke verplichting op zijn vroegst in 2024 van kracht wordt. In de Europese Unie is ook regelgeving in de maak die verplicht om algoritmes met een 'hoog risico' publiek inzichtelijk te maken.

Wet open Overheid
Op 1 mei 2022 is de Wet open Overheid (Woo) als opvolger van de Wet openbaarheid van bestuur (Wob) in werking getreden. Het uitgangspunt van de Woo is een actievere openbaarmakingsverplichting en bestaat uit een passieve en een actieve informatieverstrekking. De passieve informatieverstrekking (vergelijkbaar met het Wob-verzoek) is op 1 mei 2022 direct in werking getreden. De actieve openbaarmakingsplicht daarentegen treedt voor verschillende onderdelen gefaseerd in werking. Ook wordt met de Woo gestreefd naar het zoveel mogelijk digitaal communiceren met de indieners van verzoeken. Naast nieuwe mogelijkheden, levert dit vanuit privacy & security ook risico’s op, zodat bij implementatie betrokkenheid van de PO, CISO en FG van belang is.

Wet Aanpak Meervoudige problematiek Sociaal Domein
De Wet Aanpak Meervoudige problematiek Sociaal Domein (Wams) treedt waarschijnlijk op 1 januari 2024 in werking. In de Wet Wams wordt de wettelijke borging van de regionale meldpunten voorbereid. De Wet Wams betreft een aanpassing van de Wmo en regelt een basis voor gegevensdeling in het Sociaal Domein en een gemeentelijk meldpunt niet-acuut. Ook deze wet levert, naast nieuwe mogelijkheden, vanuit privacy & security risico’s op, zodat bij implementatie betrokkenheid van de PO, CISO en FG van belang is.

5. AANBEVELINGEN EN ACTIES

5.1 Aanbevelingen

Belang: het is belangrijk om het bewustzijn over het belang van het zorgvuldig omgaan met en verwerken van persoonsgegevens blijvend onder de aandacht te houden bij de medewerkers. Daarbij is de combinatie privacy en informatieveiligheid een vast gegeven.

Aanbeveling: voor een blijvend bewustzijn regelmatig berichten op intranet plaatsen. Ook kan met de teamleiders afgesproken worden dat de Privacy Officer met enige regelmaat of incidenteel aanschuift bij teamoverleggen om in algemene zin of aan de hand van een specifieke casus het bewustzijn over het omgaan met persoonsgegevens hoog te houden.

Vanuit informatieveiligheid blijft aandacht gevraagd worden voor het vergrendelen van het beeldscherm als de werkplek verlaten wordt. Verder is het van belang dat fysieke documenten veilig achter slot en grendel liggen en dat bezoekers tot aan de deur worden begeleid. Ook bij het thuiswerken moet worden gelet op het opbergen van documenten, omdat het niet de bedoeling is dat onbevoegden, denk aan huisgenoten, kennis kunnen nemen van vertrouwelijke informatie.

Belang: het is belangrijk om de bescherming van persoonsgegevens goed te borgen. Zowel vanuit privacyoverwegingen als gezien vanuit de beveiliging van informatie en het (be)veilig(d) omgaan met informatie, gegevens en documenten is dit van groot belang.

Aanbeveling: Waar nodig protocollen en procedures met betrekking het werken met persoonsgegevens voor afdelingen en/ of teams opstellen. Als deze zaken geregeld zijn, is de bescherming van persoonsgegevens beter geborgd.

Belang: Uit de AVG vloeit voort dat passende technische en organisatorische maatregelen moeten worden genomen ter beveiliging van persoonsgegevens. Een voorbeeld hiervan is logging en controle op de logging (monitoring) bij het gebruik van applicaties. Uit de zelfevaluatie (zie paragraaf 3.5) komt echter naar voren dat logging en monitoring nog niet voor alle applicaties is ingericht. Dat hier eventueel handhavend tegen kan worden opgetreden daar de AP, blijkt uit boetes die zijn opgelegd aan het Haga Ziekenhuis en het OLVG. Bij deze organisaties was er sprake van een datalek in combinatie met een gebrekkige logging en monitoring.

Aanbeveling: Een volgende stap in het nog beter privacy- proof maken van de gemeente Barneveld is het verder invoeren van passende technische en organisatorische maatregelen, meer specifiek logging en monitoring bij het gebruik van applicaties. Wordt dit in 2023 niet ingevoerd, dan loopt de gemeente Barneveld op dit vlak een groot risico.

Belang: Een andere passende technische en organisatorische maatregel ter beveiliging van persoonsgegevens is het op een veilige manier bewaren en verzenden van gegevens. Door het digitale werken kunnen bestanden met persoonsgegevens makkelijker (onbewust) worden bewaard op plekken waar dat niet gewenst is. Hierbij kan gedacht worden aan de persoonlijke e- mailbox en Onedrive in plaats van een vak applicatie of het zaaksysteem. Het is van belang dat er binnen de gemeente Barneveld een eenduidige lijn is waar bestanden met persoonsgegevens bewaard moeten worden.

Aanbeveling: In afstemming met stakeholder tot een gedragen werkinstructie te komen waar bestanden met persoonsgegevens moeten worden opgeslagen en op welke wijze deze gedeeld/ verzonden mogen worden met derden.

Belang: Uit een DPIA komen maatregelen naar voren die geïmplementeerd moeten worden om mogelijke risico's te mitigeren. De teams dragen zelf verantwoordelijkheid voor het implementeren van de maatregelen. Zonder deze implementatie, blijven risico's bestaan.

Aanbeveling: Er moet structureel een proces komen voor controle op opvolging van de maatregelen uit de DPIA. De PO kan deze controle uitvoeren en de FG kan vervolgens toetsen of alle mitigerende maatregelen zijn genomen.

5.2 Acties voor 2023

In de voorgaande hoofdstukken is aangegeven welke werkzaamheden in 2022 zijn uitgevoerd en in paragraaf 5.1. worden de aanbevelingen genoemd. In deze laatste paragraaf wordt nader ingegaan op de acties die hiervoor al kort genoemd zijn. In 2023 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2023 gerapporteerd zal worden.

- DPIA's: evalueren van de opgepakte en uitgevoerde van de uit de rapportages voortgekomen aanbevelingen en maatregelen. Daarna toezien op de naleving ervan.
- DPIA's: herzien en actualiseren van uitgevoerde DPIA's in verband met de 3-jaarlijkse herziening;
- Opstellen en uitvoeren van het verbeterplan Wpg;
- Continue aandacht houden voor het belang van het afsluiten van verwerkersovereenkomsten en het overzicht actueel houden. Verouderde overeenkomsten actualiseren en nieuwe overeenkomsten afsluiten met nieuwe verwerkers.
- Vervolg workshops Privacy & Informatieveiligheid voor nieuwe medewerkers.
- Op verzoek aansluiten bij teamoverleggen of afdelingsoverleggen om privacy binnen een bepaald vakgebied te bespreken.

- Vervolg opschoonacties, waarbij de wettelijke bewaartermijnen goed in acht genomen moeten worden. Bij het opschonen van documenten en (persoons)gegevens, inclusief metadata, moet niet vergeten worden dat veel medewerkers schaduwbestanden hebben in ordners en op netwerkschijven. Ook de gegevens en documenten in e-mailberichten mogen daarbij niet vergeten worden.
- Actiepunten zelfevaluatie/borging oppakken.